Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

March 2016

Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the State Office of Cyber Security, Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring, and analysis of Washington State's security posture.

The goal of the tabletop exercise is to increase security situational awareness and to facilitate discussion of incident response in as simple a manner possible; targeting a time range of 15 minutes. The exercises provide an opportunity for management to present realistic scenarios to a workgroup for development of response processes.

How to best use the tabletop exercise:

1. Modify the tabletop scenario as needed to conform to your environment.

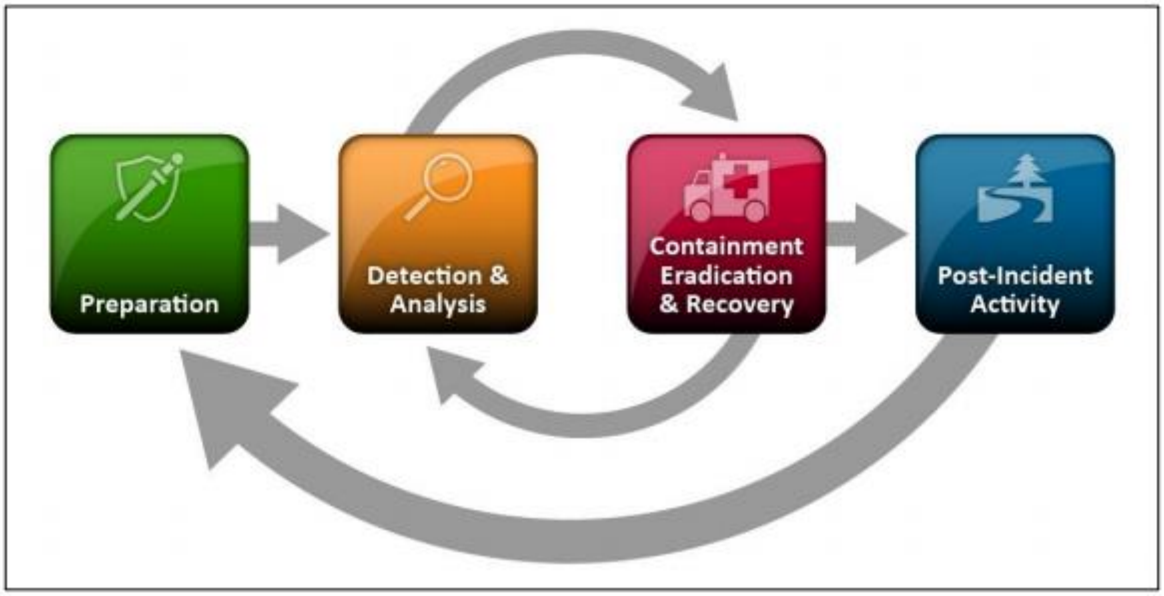
2. Engage management.

3. Present scenario to the workgroup.

4. Discuss the process to address the scenario.

5. Document the response and findings for future reference

Note: A member of the State Office of Cyber Security, Security Operations Center will be happy to facilitate this exercise with a workgroup from your agency upon request to the WaTech Service Desk at 360-753-2454.

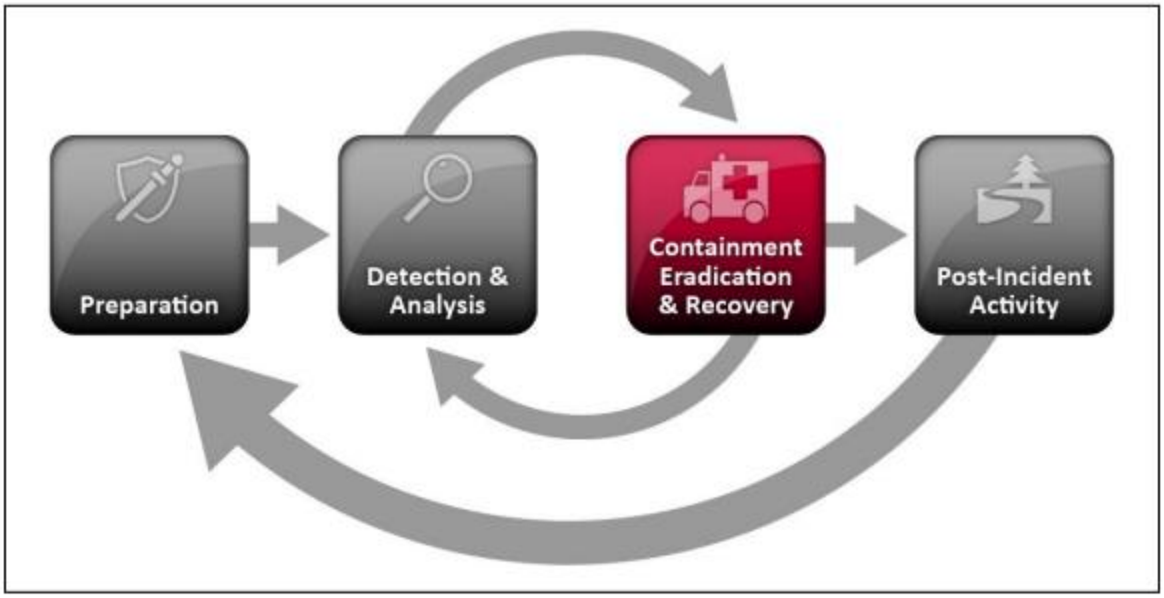


EXERCISE SCENARIO

What started off as a rather relaxing day quickly took a turn as your phone started to ring. Picking up the phone, one of your team members informs you that there seems to be a slew of incidents that have trickled up at the same time and doesn't know where to start first. Below are the events that are currently happening.

- Malware infection on multiple workstations.
- Suspicious traffic originating from an internal server to an IP address in Easter Europe.
- Hacktivist publicly announcing they have found a vulnerability on one of your websites.
- You received a notification from a federal partner that user credentials from your organization were found on Pastebin with clear-text passwords.
- An employee called the help desk claiming that their computer started acting "weird" after having plugged in a USB that was given out during an event that was attended by other staff.
- There has been a notable uptick in suspicious emails being flagged by your users and security products.
- You received an advisory informing you that there is a massive vulnerability, currently being exploited, found in the browsers used by your organization.
- A separate website is currently unavailable due to a suspected DDoS.

How do you respond?

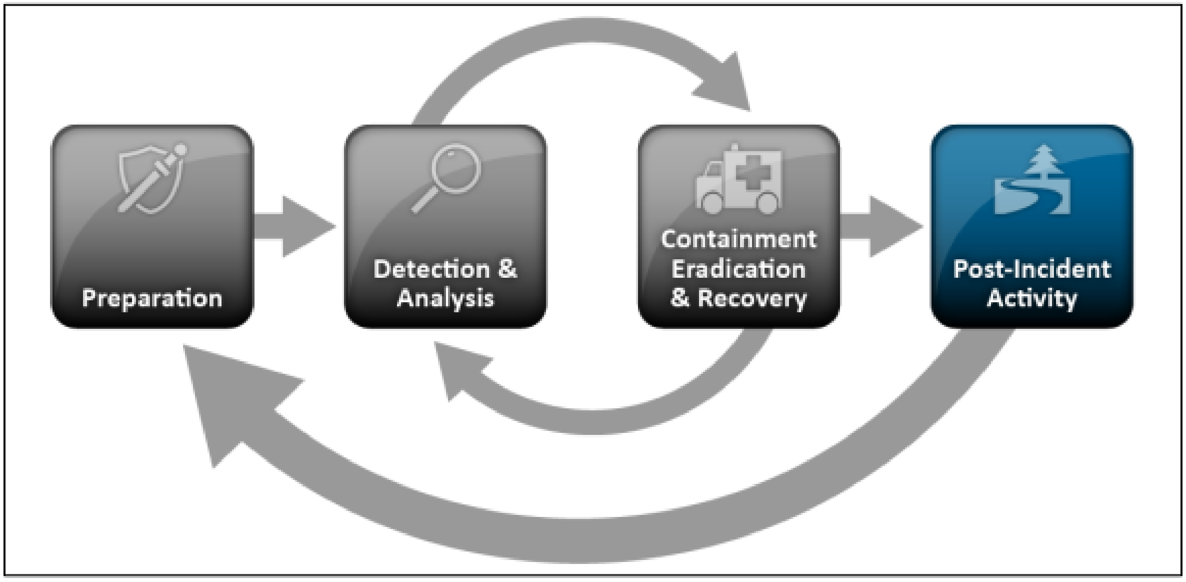


ITEMS TO DISCUSS

- How would you classify and prioritize the different incidents?
    - How can you determine the scope of the various incidents?
- Which incident do you tackle first?
    - How can you contain the incidents?
    - How can you mitigate the incidents?
    - How can you determine what were the original vulnerabilities leveraged?
    - How would you verify that the incidents have been remediated?
- What resources can you leverage internal to your organization?
    - What resources are currently missing to effectively address the incidents?
- What external resources can you leverage?
    - At what point can you leverage them?
    - How would you leverage them?
- What information would you share with partners?
- How would you track the incidents?
- Who would be informed of the incidents and when (escalations)?
    - Management?
    - Users?
    - Law enforcement?
    - MS-ISAC?

ITEMS TO REPORT

- Did communications flow as expected? If not, why?
- Were processes and procedures followed?
- Were there any surprises?
- How well did the exercise work for your organization?



CONTACT US

The State Office of Cyber Security SOC forms a focal point for the efficient reporting, containment, and recovery of security incidents.

To report a cyber-incident, contact the WaTech Service Desk at (360) 753-2454 / 1-888-241-7597.

For general questions, send us an email at soc@watech.wa.gov.

For more information, visit our site at: http://www.soc.wa.gov.

The State Office of Cyber Security, Security Operations Center (SOC) is an active member with the Multi-State Information Sharing and Analysis Center (MS-ISAC) which has been designated by the US Department of Homeland Security (DHS) as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments. Through this relationship, the State Office of Cyber Security SOC is able to leverage resources available from MS-ISAC of malware analysis, reverse engineering, log analysis, and forensics analysis in a cyber incident.

The mission of the State Office of Cyber Security SOC is to provide centralized information sharing, monitoring, and analysis of Washington State's security posture. The promotion of cyber security education and awareness to end users is critical to maintenance of a strong security posture of the Washington State network.

SECURITY OPERATIONS